# Subgroups. Lecture 2.

Let $G$ be a group. Let $H$ be a nonempty subset of $G$. We say that $H$ is a subgroup of $G$ if

(1) $\forall a, b \in H$ the product $ab$ lies in $H$;

(2) $\forall a \in H \quad a^{-1} \in H$.

If (1), (2) hold then $e = a \cdot a^{-1} \in H$.

The subgroup $H$ can be viewed as a group on its own.

Notation: $H \leq G$.

Examples. (1) $(\mathbb{Z},+) < (\mathbb{Q},+) < (\mathbb{R},+) < (\mathbb{C},+)$.

(2) $(2\mathbb{Z},+) < (\mathbb{Z},+)$, $(n\mathbb{Z},+) < (\mathbb{Z},+)$.

(3) $SL(n,\mathbb{R}) = \{A \mid \det(A) = 1\} < GL(n,\mathbb{R})$.

Question. Let $\mathbb{Z}_{\geq 0} = \{a \in \mathbb{Z} \mid a \geq 0\} = \mathbb{N} \cup \{0\}$.

Is $(\mathbb{Z}_{\geq 0}, +)$ a subgroup of $(\mathbb{Z}, +)$ ?

## Generators.

Let $G$ be a group. Let $a_1, \ldots, a_n \in G$.

Let $a_1^{-1}, \ldots, a_n^{-1}$ be the inverses of the elements $a_1, \ldots, a_n$ respectively. Let $H$ be the set of all products of elements

$a_1, \ldots, a_n, a_1^{-1}, \ldots, a_n^{-1}$

$$H = \{a_{i_1}^{\pm 1} \cdots a_{i_k}^{\pm 1}, e\}$$

Then $H$ is a subgroup of $G$.

Indeed,

$$a_{i_1}^{\pm 1} \cdots a_{i_k}^{\pm 1} \cdot a_{j_1}^{\pm 1} \cdots a_{j_t}^{\pm 1}$$

is a product. What about inverses ?

$$(xy)^{-1} = y^{-1}x^{-1}$$

Indeed: $xy \cdot y^{-1}x^{-1} = e$.

$$(x_1 \dots x_k)^{-1} = x_k^{-1} \dots x_1^{-1}.$$

Hence,

$$\left(a_{i_1}^{\pm 1} \dots a_{i_k}^{\pm 1}\right)^{-1} = a_{i_k}^{\mp 1} \dots a_{i_1}^{\mp 1}$$

We say that the subgroup $H$ is <u>generated</u> by the elements $a_1, \dots, a_k$.

<u>Notation:</u> $H = \langle a_1, a_2, \dots, a_k \rangle$.

If $G = \langle a_1, \dots, a_k \rangle$ then we say that $a_1, \dots, a_n$ generate $G$.

<u>Cyclic groups</u> = generated by one element.

## Cyclic Groups.

**Theorem.** Every cyclic group is isomorphic to $(\mathbb{Z}, +)$ or to one of the groups $(\mathbb{Z}(n), +)$, $n \geq 1$.

**Proof.** Let $G$ be a cyclic group, $G = \langle a \rangle = \{a^i, i \in \mathbb{Z}\}$. Consider the infinite (in both directions) sequence

$$\ldots, a^{-2}, a^{-1}, a^0 = e, a, a^2, \ldots$$

**Case 1.** All these powers are distinct.

Consider the mapping

$$\varphi : \mathbb{Z} \to G, \quad \varphi(i) = a^i.$$

Since all the powers of the element $a$ are distinct it follows that this mapping

$\varphi$ is a bijection,

$$\varphi(i+j) = a^{i+j} = a^i \cdot a^j$$

Hence $\varphi$ preserves multiplication. Hence $\varphi$ is an isomorphism.

Case 2. Not all powers $a^i$ are distinct.

There exist integers $p < q$ such that

$$a^q = a^p$$

Multiplying the equality by $a^{-p}$ we get

$$a^{q-p} = e$$

So, there exists a positive number $m \geq 1$ such that $a^m = e$. Let $n$ be the smallest positive number such that

$$a^n = e.$$

Remember : in every nonempty subset of $\mathbb{N}$ there is a minimal element.

This number $n$ is called the order of the element $a$, it is denoted as $n = |a|$.

Now,

$$G = \{ \cdots a^{-2}, a^{-1}, e, a, a^2, \ldots, a^{n-1}, e, a, a^2, \ldots \}$$

$$a^{-2} = a^{n-2} \qquad a^{-1} = a^{n-1}$$

The sequence is periodic.

$$G = \{ \ldots, \underbrace{e, a, a^2, \ldots, a^{n-1}}, \underbrace{e, a, a^2, \ldots, a^{n-1}}, \ldots \}$$

$$= \{ e, a, \ldots, a^{n-1} \}$$

Now $\mathbb{Z}(n) \xrightarrow{\varphi} G$, $\varphi(i) = a^i$ is an isomorphism.

Theorem. Every subgroup of a cyclic group is cyclic.

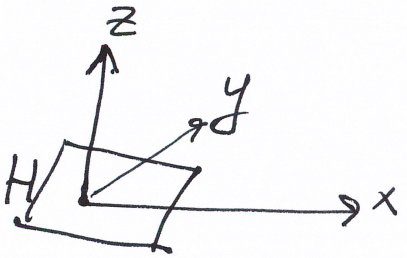
We won't prove this theorem.

## COSETS.

Let $H \leq G$, $H = \{h_1, h_2, \dots\}$, $g \in G$.

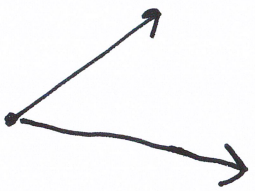
**Definition.** The subset $gH = \{gh_1, gh_2, \dots\}$ is called a **left coset** of the subgroup $H$.

**Example.** $G = (\mathbb{R}^3, +)$

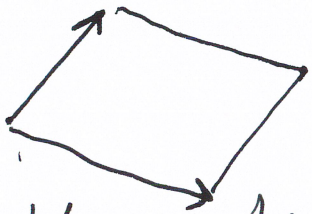



$H$ = plane that passes through the origin $O$.

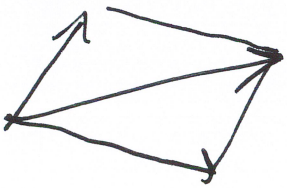
Then $H$ is a subgroup of $G$. If vectors



lie on a plane then the whole parallelogram



lies on the plane and the sum



lies on the plane.

$H \to gH$ (here $g + H$) is a parallel translation.

A coset = a plane that is parallel to $H$ but may not contain $0$.

Lemma. Two cosets either do not intersect or coincide (like parallel planes).

Proof. Let $g_1 H$ and $g_2 H$ be left cosets.

Suppose that $g_1 H \cap g_2 H \neq \emptyset$,

$$g_1 h_1 = g_2 h_2 \; ; \quad h_1, h_2 \in H.$$

Then $g_2 = g_1 h_1 h_2^{-1}$. Hence for any $h \in H$

$$g_2 h = g_1 \underbrace{h_1 h_2^{-1} h}_{\uparrow H} \in g_1 H.$$

We proved that $g_2 H \subseteq g_1 H$. Similarly

$g_1 H \subseteq g_2 H$. Hence $g_1 H = g_2 H$. ∎

Lemma. $G = \cup$ (all left cosets of $H$).

Proof. An arbitrary element $g \in G$ lies in the coset $gH$ since $H \ni e$. ∎

Lemma. All cosets contain the same number of elements, $|gH| = |H|$.

Proof. The mapping $H \to gH$, $h \to gh$, is a bijection. Hence $|gH| = |H|$. ∎

Let $g_1 H, \ldots, g_s H$ be all distinct cosets of $H$. The number $s$ is called the index of $H$. It is denoted as $|G : H|$.

Remark. $|G : H|$ may be infinite.

In the same way as above we can define right cosets $Hg$ and the right index = # of all distinct right cosets of $H$.

Exercise. Prove that the left index of $H$ = the right index of $H$.

Hint: Consider the mapping $G \to G$, $x \to x^{-1}$, that maps left cosets into right cosets.

Lagrange Theorem. Let $G$ be a finite group, $H < G$. Then $|G| = |H| \cdot |G:H|$.

Proof. The set $G = g_1 H \dot\cup g_2 H \dot\cup \dots \dot\cup g_s H$ is a disjoint union of $s = |G:H|$ subsets, each containing $|H|$ elements. Hence $|G| = |G:H| \cdot |H|$. ↓

Another Lagrange Theorem. For an arbitrary element $a \in G$ $a^{|G|} = e$.

Proof. Consider the cyclic subgroup $H$ generated by the element $a$,
$H = \{e, a, a^2, \ldots, a^{n-1}\}$, where $n = |a|$.
We have $|H| = n$. By Lagrange's Theorem
$|G| = |a| \cdot |G:H|$, hence

$$a^{|G|} = (a^{|a|})^{|G:H|} = e^{|G:H|} = e. \quad \downarrow$$

Computational value. Given a group $G$ and an element $a$ find $a^{-1}$. How do we do that? Try all elements $x \in G$ and check if $xa = e$?
No, we compute $a^{|G|-1}$, which may be easier.

# Number Theory Applications.

Let $p$ be a prime number.

**Small Fermat Theorem.** For an arbitrary integer $a$ the number $a^p - a$ is divisible by $p$.

**Proof.** If $a$ is divisible by $p$ then there is nothing to prove. Suppose that $a$ is not divisible by $p$,

$$a = p \cdot q + r, \quad 1 \le r \le p-1,$$

$$a = r \bmod p.$$

By Lagrange's Theorem we proved earlier that $r^{p-1}$

$\mathbb{Z}(p)^* = \{1, 2, \ldots, p-1\}$ is a group with respect to multiplication, $|\mathbb{Z}(p)^*| = p-1$.

By $r \in \mathbb{Z}(p)^*$. By Lagrange's Theorem $r^{p-1} = 1$ in the group $\mathbb{Z}(p)^*$. Hence $r^{p-1} = 1 \mod p$ and $a^{p-1} = 1 \mod p$.

Therefore $a^p = a \mod p$. ∎

Wilson's Theorem. $(p-1)! = -1 \mod p$.

Proof. Again consider the group $\mathbb{Z}(p)^*$. All elements in $\mathbb{Z}(p)^*$ "go in pairs": an element and its inverse.

Example. $p = 7$, $\mathbb{Z}(7)^* = \{1, 2, 3, 4, 5, 6\}$

There is only one nonidentical element in $\mathbb{Z}(p)^*$ that is equal to its inverse. $a^{-1} = a$ means $a^2 = e$, $(a-1)(a+1)$ is divisible by $p$. Since $a$ is a nonidentical

element $2 \le a \le p-1$, $1 \le a-1 \le p-2$, $a-1$ is not divisible by $p$. Hence $a+1$ is divisible by $p$, $a = -1 \bmod p$, $a = p-1 \bmod p$.

In the example above: 6.

This is the only element that is not cancelled in $(p-1)! = 2 \cdot 3 \cdot 4 \cdots (p-1)$, so

$(p-1)! = p-1 \bmod p = -1 \bmod p$. ∎

## Homomorphisms.

Let $G_1, G_2$ be groups. A mapping $\varphi: G_1 \to G_2$ is called a homomorphism if it preserves multiplication, i.e.

$\forall a, b \in G_1$

$$\varphi(ab) = \varphi(a)\varphi(b).$$

Let $\varphi: G_1 \to G_2$ be a homomorphism.
Let $e_1, e_2$ be identity elements of the groups $G_1, G_2$ respectively.

Exercise. 1) $\varphi(e_1) = e_2$.

2) $\forall a \in G_1 \quad \varphi(a^{-1}) = \varphi(a)^{-1}$.

Examples. 1) Every isomorphism is a homomorphism,

2) $(\mathbb{Z}, +) \to \mathbb{Z}(n)$, $a \to$ remainder of $a$ mod $n$

3) $GL(n, \mathbb{R}) \to (\mathbb{R} \setminus \{0\}, \cdot)$, $A \to \det(A)$ is a homomorphism (indeed: $\det(AB) = \det(A) \cdot \det(B)$).

## Direct Products (Sums) of Groups.

Let $G_1, \ldots, G_n$ be groups. Consider the set of $n$-tuples

$$G = \{(a_1, a_2, \ldots, a_n) \mid a_1 \in G_1, a_2 \in G_2, \ldots, a_n \in G_n\}.$$

we define the multiplication

$$(a_1, a_2, \ldots, a_n)(b_1, b_2, \ldots, b_n) = (a_1 b_1, \ldots, a_n b_n)$$

With this multiplication $G$ becomes a group.

Associativity follows from associativity of multiplications in $G_1, \ldots, G_n$.

Identity element : $(e_1, e_2, \ldots, e_n)$, where $e_i$ is the identity element of $G_i$.

Inverse : $(a_1, a_2, \ldots, a_n)^{-1} = (a_1^{-1}, \ldots, a_n^{-1})$.

Notation: this group is denoted as $G_1 \times G_2 \times \cdots \times G_n$ and called the direct product of the groups $G_1, G_2, \ldots, G_n$.

If the groups $G_1, \ldots, G_n$ are abelian and we use $+$ instead of $\cdot$, then we talk about the direct sum and denote $G = G_1 \oplus \cdots \oplus G_n$.

For every $i$, $1 \le i \le n$, the subset

$$\{(e_1, e_2, \ldots, \underset{i}{a}, \ldots, e_n) \mid a \in G_i\}$$

is a subgroup of $G_1 \times G_2 \times \cdots \times G_n$. This subgroup is isomorphic to $G_i$. So, we can say that $G_i$ is a subgroup of $G_1 \times \cdots \times G_n$.

Important theorem that we leave without a proof:

Theorem. Every finitely generated abelian group is isomorphic to a direct sum:

$$\mathbb{Z} \oplus \cdots \oplus \mathbb{Z} \oplus \mathbb{Z}(n_1) \oplus \mathbb{Z}(n_2) \oplus \cdots \oplus \mathbb{Z}(n_s),$$

$$n_1 \mid n_2,\ n_2 \mid n_3,\ \ldots,\ n_{s-1} \mid n_s.$$